Data protection between property and liberties

Poullet, Yves

Published in:
Amongst friends in computers and law. A collection of essays in remembrance of Guy Vandenberghe

Publication date:
1990

Document Version
Publisher's PDF, also known as Version of record

Data Protection between Property and Liberties
A Civil Law Approach[1]

Yves Poullet

1. Certain authors in civil law countries assert a suggestion that the 'right of property' can be viewed as a diagram of the prerogatives which are granted by the Data Protection regulations to the individual about his 'computerized image'. Our intention is thus for the first time (Part I) to examine this assertion or suggestion. But this analysis will bring us to a second proposition, radically different. The debate about privacy considered in terms of property leads on to another debate much richer and more comprehensive; that is to say the debate about our freedoms (Part II). The notion of freedom viewed as a self-controlled 'autodetermination' exercised by individuals seems to us more fit to enlighten present debate and solutions around Data Protection.

Part I. Property as an Explanatory Basis for Data Protection (D.P.)

2. In a famous article, the French author P. Catala asserts: "(D.P. regulations) grant to individuals important prerogatives on nominative data, notably, rights of access and correction. The same regulations enable individuals to refuse the recording of data about themselves in a data file and entitle them, to require information from those who gather information about themselves. All these innovations can be considered as ways to protect the 'supplier' of the nominative data, that is to say the individual. Indeed, these are prerogatives of the 'ius in rem'. Implicitely, these new rights granted to the data subject are a clear acknowledgment that nominative data belong to the individual concerned, the legitimate owner, who in this capacity is allowed to check their good use and their veracity".

The author develops his argument as follows. "In our opinion, the data protection granted to individuals by the Privacy regulations means a right on nominative data rather than a right to this information".

So, according to Catala, the framework explaining Data Protection rights is comparable to that explaining the 'ius in rem'. The 'ius in rem' is defined in civil law countries as an individual right characterized by a direct and immediate

1) This paper is a revised version of the report presented at the Colloquium "Nouvelles technologies et propriété" in Montreal (November 1989). The original report in French will be published by the University of Montreal (ed. E. MacKaay).

prerogative regarding goods, especially in this case, on immaterial goods: the nominative data. This imposes a duty of abstention on everyone, derived from the obligation to respect this prerogative.

At first glance, the notion of 'privacy' that is to say a 'private life that would be our own property' as opposed to the one of public life seems to regard the right of property as an explanation of the right to the protection of the data belonging to this private life.

In order to summarize the reasoning, it can be asserted that

a. the individual is in a privileged relationship with regard to nominative data concerning him;
b. this relationship can be enforced against everyone:
   either when the data subject is authorized to veto the collection of certain minimal nominative data (see infra no. 3), the absolute exclusive right comparable with the property is granted to the data subject by the D.P. regulations;
   or when the data subject as regards the other nominative data only has the right to inspect, check and correct his data, or 'dismembered' 'ius in rem' is granted to the data subject insofar as the exercice by others on property in the nominative data is deeply limited by certain prerogatives devoted to the registrered person;
c. the data may be viewed as intangible goods like an artistic work.

More precise arguments are given in order to sustain this thesis: regulations on sensitive data (A) and the content of the rights devoted to the data subject (B) can be considered as direct consequences of the analogy between D.P. rights and property.

A. The Regulations on Sensitive Data

a. The Thesis

3. Private life is defined by WARREN and BRANDIES (1870) as a "right to be let alone", in other words, according to RAVANAS, a "secret field of the life for which he can keep from third persons". This approach is adopted by the D.P. regulations, which enumerate a list of data called "sensitive data" or "hard case of the private life" which in themselves should be considered as a matter of intimacy. The data subject as an owner has the absolute right to exclude everybody for collecting, storing and disseminating these kinds of data. So, under the Council of Europe Convention (art. 6) "personal data which concerns the social origin, the political opinions, the religious convictions and philosophical convictions, as well as data concerning the health, the sexual life and criminal sentences ..." may not be recorded. The lists of these data in some countries draw around the individual a closed and protected field, a 'Candide's garden'. The owner of those data has the right to forbid to anybody else from sharing of this ownership.

b. Refuting this thesis

4. The property right cannot be used to explain the right of the individuals regarding data pertaining to him.

Firstly, a property right is defined primarily as a right to own a good. The notion of 'restricted data' excludes precisely every disposition of the data even considered as intangible goods.

Secondly, some 'restricted data', considered as 'hard core' of the private life: notably race, philosophic and religious opinions, are public, open to anyone. Who is able to hide his race and would a trade union militant wish to avoid mentioning his trade union membership?

5. So it seems that it is not the privacy – a vague and undefinable concept but the fear of discriminatory practices which justifies the severe restrictions a priori on the collection and storage of such data.

In other words, it is the protection of our inalienable liberties, to express our opinions, to lead a sexual life according to our own ways and not the protection of our private life opposed theoretically to a public life which justifies the specific protection of some nominative data. If the explanation is such, we have to agree with SIMITIS that the list of restricted data may not be enlarged and overall that the 'public interest' or the freedom of third persons could justify cases where the so-called restricted data may be stored. Finally the prohibition might be removed if the person, with full knowledge and freely, does accept the storage by a third party of his data a priori sensitive.

6. Lastly, some reflections about article 26 of the French Data Protection Act (whose content is considered by CATALA as an argument in favour of his thesis) strenghten our conviction on the necessity to leave the debate 'Information et vie privée' and to prefer this oneInformatique et libertés' (by the way, title of the French D.P. Act).

Art. 26 of the French Act grants to the data subject the right to veto, for legitimate reasons, the recording of data pertaining to him in another's file.[2]

Against this explanation, two arguments are given:

- the French legal provision is exceptional. No similar provision can be found in other data protection legislations.
  However, the right of third parties to store nominative data may be strongly limited but in no way, in the other countries, is the absolute priority of the right of the data subject asserted over the right of the third parties to collect and store information about this data subject.
- the French legal provision does not grant an absolute right, even if apparently this seems to be the case, but a functional right, that is to say a

2) The CNIL, in its 'ten years' report, denotes that such right means the most brilliant and tangible manifestation of the right of everybody to control his own data.

right limited in function by its purpose.

The C.N.I.L. report, already quoted, contains the following comment: "provided that legitimate reasons are not legally defined, their acknowledgment is dealt with on a case by case basis in the exercise of the discretion of the courts." The report adds: "in most of the cases, in the public sector, this right (to refuse the storage by third parties) does not exist."

7. To summarize, art. 26 of the French Act does not consecrate a direct and immediate right of a data subject in relation to such data. Rather, in particular cases where the collection of information by third parties creates some fears for the freedom of this data subject, this provision makes the data subject able to request that for reasons of his legitimate private interests the right of the third parties to the data will be limited.

The role of the judge is to balance the interests or freedoms, on the one hand of the data subject and on the other hand of the third party.

In other terms, art. 26 leads to a reflection more fundamental than this one about the existence of a private life. This provision demonstrates that in order to solve the D.P. debate it is absolutely necessary to balance different opposing liberties in a given context.

That is the meaning of our second thesis.

PART II. THE ACTUAL RIGHTS AND INTELLECTUAL PROPERTY RIGHTS AS AN EXPLANATION OF THE RIGHTS OF THE INDIVIDUAL IN RESPECT OF DATA HELD BY THE THIRD PARTY

a. The Thesis

8. If the idea of a right of property applied to data cannot resist analysis, at least we should, according to some, recognize that the prerogatives accorded by data protection legislation to the data subject are curiously parallel to those which characterize 'iura in rem' and intellectual property rights. Their common characteristic resides in a direct and immediate right pertaining to a property which is enforceable against all third parties, including the nominal owner of that property. The author of a literary or artistic work may, after the completion of his work, specifically in the name of his right of intellectual property, oppose any deformation of the expression of his personality, or any unfaithful or unauthorized reproduction of his work. Don't we see the same principles applied to the protection of data, when such is traceable to an actual person on file? This is done through the right of access, the right to control the correctness and completeness of such information and whether it is up to date, during filing, processing or transmission; through the right of pursuit (note the expression, borrowed from the terminology of real right), the right to track contentious data through several hands that may possess it in order to insist, if the case demands, on its correction and by the principle of pertinence, i.e. that

the restrictions on the destination of the data be respected.

9. The seductive parallel between 'ius in rem' or intellectual property rights and those devolving from data protection legislation, resides in the idea of there being an identical basis in law to that described in our analysis of rights of property as the foundation of the right of privacy: that there exists between the individual and data concerning him a direct and immediate proprietary relationship. In other words, the first rational step is to make the idea of personal data objective, which is, in fact, no more than an extension of one's personality and, as such, is inseparable from oneself, in order to give it, in a second step, one or more bearers who share rights to it as information. Thus, a bank which collects such information and inscribes it on a data memory card, thereby enabling access to certain banking services, could be called the owner of that information, on condition that it respects the real rights of the person recorded.

b. Refuting this Thesis

10. The comparison can be easily refuted and its analysis invites us to tread a path which escapes the domain of real or assimilated rights to rejoin that of rights of personality or liberties.

The right of the data subject to require from the holder of the data file the non-alteration, the rights of correction and respect for the destination of his nominative data are curiously similar to the prerogatives which moral rights (still qualified as extrapatrimonial) confer upon an artist with regard to his works. 'Moral right' says the French Cour de Cassation (Cass. 6 July 1965, G.P., 1965, 2, 126) "which is held by the author of a work of art, enables him to make sure that his work, once it has been released to the public, is not misrepresented or mutilated" (see in this respect, German jurisprudence, Reichsgericht, RGZ, 79, 397, 399). The analogy of the rights of a person filed with untransferable extrapatrimonial rights, strictly personal and inalienable, as opposed to rights of estate, is easily justifiable. Data protection legislation insists on the personal nature of the right of access, forbidding all transfer, assignment or collective exercising of that right, and certain legislations severely punish any abuses in relation to the data by a third party, such as forcing the bearer of the right of access to exercise that right against his will.

Upon any nominative data, as upon a work of art, would be superimposed two layers of rights, both equally absolute and universally indefeasible; that of the holder of the file essentially patrimonial, he is the proprietor of the information medium in which the nominative data is stored and that extra-patrimonial and inalienable right of the information donor.

11. Jurisprudence has from time to time busied itself with the relationship that exists between the moral right of an author and the patrimonial rights over a work of art exercised by another. Thus, in the judgement pronounced in LECOCQ, a composer of the early twentieth century, the Court of Cassation (Cass. 25 June 1902, D.P., 1903, I, 5, note A. COLIN) clearly distinguished economic exploitation, such as royalties, one attribute of authors' rights, from the moral right, another attribute of authors' rights. In this case, the patrimonial rights of economic exploitation pertained to the estate and formed part of the joint property of the LECOCQ marriage, subsequently dissolved by divorce. However, according to the court, this placing in common of the monopoly on exploitation had no influence on the right of the author, inherent to his own personality, to ultimately submit his creation to modification, or even to suppress it, inasmuch as such actions were not undertaken with the intention of making difficulties for his former wife.

12. Among the prerogatives of an author's moral right, legal doctrine distinguishes two types. The first pertains to prerogatives having precise content, such as the right of paternity: each author is entitled to demand to see his name appear on any work of which he is the author. The second type of prerogative has no precise content, such as the right to withdraw a work from publication, or to the non-alteration of a work. Such prerogatives cannot be exercised in such a precise manner, their correct interpretation depending rather on the understanding of the judge, who must balance the seriousness of the affront to the author's personality against the rights of another. Such prerogatives are not absolute, but may conflict with other rights or issues. The owner of a work of art may decide to destroy it, or to exploit it in such and such a way. The author may not invoke an affront to his personality, except in those rare cases where the actual nature of exploitation is in manifest discord with his known principle (as when an author well-known for his pacifist ideals has his work used to promote the sale of weapons). To give another example, it is clear that the principle of the inviolability of domestic privacy is not comparable with that of an author being able to monitor the respect due to his work at the home of the owner (Paris 6 July 1975, G.P., 1965, 2, 126). In the LECOCQ case, the judge verified whether the exercise of the right of personality did not represent an abuse once the author opposed the legitimate exercise by another of patrimonial or proprietory rights over a work of art.

In conclusion, as RIGAUX observes (T.II, P. 178) with regard to these peculiarities and conflicts, "it is contradictory to contend that two people can be in possession of a prerogative constructed on the basis of property rights, thereby attributing to the one as well as the other the control of a right whose extent each may define as he chooses."

In reality, it is a matter of two prerogatives of differing nature, one concerning the property of personality, according to the same author, and the other, the civil rights of patrimony.

Conclusions

13. In view of the preceding considerations, the thesis of property rights or real rights as a justifying foundation for data protection legislation seems to us to be at once erroneous, dangerous and incapable of explaining the evolving debate over data protection.

Each term of this proposition can be justified as follows:

- *the thesis is false* inasmuch as it pretends to isolate the data from its context in order to define it as the object of a real right. However, even in the case of sensitive data, data protection legislation does not attribute a value to the data itself, but views it in its functional context, that is to say, with regard to the intended ends of its recording or its processing. In this way, data protection legislation tends first and foremost to control the nature of and the right to information gathered by holders of the file rather than to recognize, a priori, a direct connection between a person and data concerning him.
- *the thesis is dangerous* inasmuch as, by placing the right to protection in the territory of real rights, it gives rise to the idea of a possible commercialization of that right (RODOTA). In this respect, the American debate on the regulation of cable TV is in point. In 1982 the president of the FCC, in a report titled: "Economics and Privacy in Telecommunications", justified the uselessness of all specific 'privacy' regulation concerning the recording of cable use data (choice of programme, duration of attention, etc), by affirming that the competition in this sector leads cable operators to offer those who wish to cooperate for money guarantees that this data will be treated confidentially. In other words, according to POSNER, 'privacy', like any other marketable property, can be bought or is at least negotiable.

  The opponents of this position (GARDNER and WHITE, WESTIN) note that:

  - the rules of the game cannot apply where there already exists such a distortion of powers between potential contracting parties;
  - the debate exceeds the question of the free disposition of a so-called patrimonial property to rejoin that of a public debate on the protection of an essential public liberty, that of opinion, in this case revealed by the choice of cable programmes.
- *the thesis, finally, is incapable of taking into account regulatory evolution*, inasmuch as the right of free and informed consent required by recent legislation in response to new technologies, such as RNIS or data memory ('smart') cards, is not justified by the existence of inherently new data but rather by the degree to which technological evolution has created new forms of information circulation, requiring extra guarantees for citizens liberties.

In other words, to adopt the conclusions of the IBI, "the comparison between the right to confidentiality in private life, demanded by twentieth century man, and the law of private property, proclaimed in preceding centuries as a 'natural law' and with which one may approach the 'right to privacy' such as it was understood by its original authors, WARREN and BRANDEIS, has been proposed and discussed many times. Certainly, it is a suggestive analogy, but one which does not establish precise parallels... Given the current social conditions, it concerns more the area of political rights exercised by the citizen towards public (and, we must add, private) authority, which has developed into an 'information power', inasmuch as it has become the custodian and administrator of highly complex electronic archives. It is therefore a matter of liberty, not of an aristocratic liberty suited to a privileged few desirous of being left in peace, but of a democratic liberty which concerns everyone, in social relationships which have taken on a new form as a result of our technological civilization."

As early as 1974, RODOTA wrote in a similar vein: "Those who are able to comprehend the true nature of the debate are aware that it can no longer be expressed in terms of the classic theme of privacy versus external encroachment, but that as a result of considerable qualitative change, the problem of the confidentiality of private life is to be viewed in the context of contemporary power structures, structures of which information constitutes an essential component. To summarize this evolution, one must stress that the right to a certain intimacy is constantly losing ground to the advantage given to the individual by the possibility of exercising control over the communication of information concerning him."

I. THE THESIS

A. The decision of the German Federal Constitutional Tribunal (Bundesverfassungsgericht) on the demographic census

14. The law on demographic census and the methods by which such are carried out was the object of an appeal to the above tribunal on the part of the German 'Greens', an ecological political party. The judgement of 15 December 1983 went in their favour. It ordered that the programme of statistical enquiry be complemented by certain measures pertaining to procedure and security, and declared as unconstitutional any communication of the data gathered. The rationale for this decision was the threat to those 'general rights of personality' progressively clarified by the German Federal Tribunal on the basis of articles 1 (1) (the inalienable nature of human dignity), and 2 (1) (right to the free development of the personality) of German constitutional law. "The Federal Tribunal considers the '*right to self-determination in matters of information*' (Informationelle Selbstbestimmungsrecht) to be an integral part of the general rights of the individual. The value and dignity of the human individual acting in freedom as a member of a free society are the essential principles of fundamental law." (BURKERT, 1985)

15. This right of self-determination, which is the right of every individual to be in control of the image of himself which he projects upon society, is particularly endangered by current and future possibilities in information processing. It cannot, however, be understood in an absolute way. The individual, according to the constitutional Court, does not exercise unlimited sovereignty over matters concerning him. His personality develops in the bosom of society, he cannot live without communicating. Information, even nominative, is a representation of social reality, which is not uniquely the property of the person concerned. The fundamental law resolves the 'individual-society' dichotomy by considering the individual as an entity joined to and inserted into society. This is why, in principle, the individual must accept restrictions on his 'right to self-determination', and this in favour of the preponderant general interest.

B. Individual Liberty, True Foundation

16. So, the right to self-determination constitutes the true foundation of data protection legislation. But in fact, according to RIGAUX (1988, 578), what is this right of self-determination, if not a liberty?

RIGAUX's thesis is to show precisely that the protection of privacy, and beyond that, of the property of personality, is a matter directly of individual liberty, and that *any confusion or comparison with classic subjective patrimonial rights only serves to obscure the issue*. "The property of personality opens out onto a field far vaster than any which has hitherto been ascribed to it. It is certainly not a matter of reinforcing all the patrimonial rights of an ectoplasm entitled to rights of personality, but rather of readjusting the rules that apply to such rights in their entirety, in a manner which takes the dignity and personality of private individuals within the meaning of the law more into account." (RIGAUX, 1988, 578)

According to the author, the right to data protection cannot be understood by reducing the issue to the recognition of a subjective right qualifying the right to privacy. In fact, subjective rights are characterized by the way in which they confer upon their bearer a controlling relationship towards a determined object: "It is part of the nature of such rights that they confer upon their bearer precise prerogatives accompanied by the right of exclusivity." (RIGAUX, 575) **"Does a 'private sphere' exist which can be made the object of exclusive subjective appropriation and, as such, be shielded from any third party involvement? Is the control of such a private sphere protected by an unconditional subjective right analogous to the right of property? The impossibility of defining such a sphere other than by tautology imposes on such questions an answer in the negative. The search for some hard kernel which one might call 'intimate privacy' is no less doomed to failure. Even the most grave inroads on privacy, which one may presume to be illicit and which generally have that character, lose it in exceptional circumstances. It can occur that the**

members of society at large have an interest in being informed of that which may be part of the subject's intimate life, or that the latter is unable to produce a sufficiently constraining interest to resist such an exposure, where the author of the exposure is not making any illicit use of his liberty."

C. Consequences

17. RIGAUX's thesis puts the following points in evidence:

a. Liberty and human dignity, the ultimate bedrock of data protection legislation, justify, with regard to the specific danger that data processing represents, the consecration of precise subjective rights, permitting the individual the necessary minimum means to ensure his right of self-determination. The German constitutional Court has stated: "Faced with the danger already described emanating from the use of automatic data processing, the legislator must take more ample precautions than previously with regard to the organization and procedure of data processing, with the goal of preventing any violation of human rights." From this perspective, the consecration of certain specific subjective rights will be justified, which one might group under the heading 'rights of access'. The analogy with the right of paternity, a specific subjective right arising from non-patrimonial attributes conferred upon the author, may be evoked at this point. It is a matter of showing that this subjective right is capable of taking on new forms, with regard to new dangers arising from, or the particularities of, the new techniques.

b. Liberty and human dignity oppose certain other liberties, those of other individuals, other interests, and notably the public interest.

"Liberty rather than right, Selbstbestimmungsrecht must be reconciled with the equally recognized liberty of al other rightful subjects. Fundamental rights are sometimes in conflict with one another. Finally and above all, the Bundesverfassunsgericht has not recognized, in the right to unfettered development of the personality, an unlimited range. Each time that is has been deemed necessary, the constitutional legal authority has reminded us that the individual is a person inserted into society: this may, in the public interest or to safeguard the rights of another, impose upon its citizens obligations or abstentions which limit their natural liberty" (RIGAUX, 1988, 485). Data protection legislation includes defining certain criteria which permit us to delineate clearly the right of the holder of the file to information as an expression at one time of his entrepreneurial right in the private sector, at another time of his role, in the public sector, of guardian of the public interest.

c. Finally, RIGAUX's thesis obliges us to emphasize the necessity of defining the balance between conflicting interests in an evolutive manner and

to deepen ourselves in the role of the institutions charged primarily with helping to define this balance in an evolutionary context.

Each of these points will be the object of specific comment.

II. THE RECOGNIZED EXPLANATORY BASIS FOR DATA PROTECTION JUSTIFIES NEW SUBJECTIVE RIGHTS FOR PERSONS ON FILE

A. Explanation and Contents

18. RIGAUX writes (1988, 558): "In the modern social state, the inviolability of human dignity can no longer be guaranteed by LOCKES obsolescent model: liberty and property. It would be going too far to say that the new rights have been conceived in opposition to property, but they exercise a complementary function, or one of substitute. In order that the right of property remains tolerable, in view of the considerable inequalities that it entails, it was necessary to institute either new subjective rights, or the illusion of such".

Cannot the *right of access*, in its various facets granted to the person on file, be considered as a *new subjective right*, that is to say, as the complement or rather corollary that renders the preponderance of power conferred by data processing technology on its administrators somehow tolerable? The modification, both of a qualitative and quantitative order, of the informational value of an item of nominative data, a modification obtained by data processing itself, as well as by the non-transparence of information circuits, demands the recognition for the person filed of new subjective rights, grouped together under the heading 'right of access'.

19. **To recap, the right of access may be defined as a right of the person on file to participate in the formation of the image others make of him.** This right did not in the past necessitate the erection of particular subjective rights, because the circulation of nominative information could be easily kept under control in a traditional society. This is certainly no longer the case nowadays.

One example drawn from everyday life will suffice to demonstrate what we mean. Up till recently, cash represented the most common form of payment. The informational value of a cash payment is about zero, and the salesman, unless he knows the identity of his customer, can only with difficulty establish a correlation between a certain individual and a certain expenditure. In any hypothesis, the buyer can know, a priori, the people (e.g. neighbours) to whom the information will be transmitted. In the case, however, of an electronic sales terminal, the sale acquires an informational value out of all proportion to that of the cash payment. The use of electronic terminals informs the banker, a third party to the transaction, of the identity not only of the buyer, but also of the shopkeeper, plus the value and nature of the sale. The shopkeeper obtains information on the banking relationship of his customer as well as on his credit line value. The use of computer systems for the processing of such infor-

mation further increases their informational value, since the cross-checking of the various primary information thereby obtained, and its comparison, rapidly permit data administrators to build up a precise image of a client's habits of consumption, of his movements, and of the relative importance of each of his expenditures. "Even cultural and artistic tastes become suddenly transparent through the medium of libraries, theatres and concert halls. Briefly, by each individual transaction, the credit card user is revealing to a third party, who has not asked his permission, his personal tastes and opinions, his projects and his future expenses, taking into account his overall social standing." (LEMASSON, 1988)

20. Classically, West European legislation has envisaged the right of access under the following aspects:

- firstly, at the moment of information gathering, it is the right of the person about whom information is recorded to know why, and by whom he is being interrogated, whether a response is obligatory or not, and to what final ends the information may be used;
- equally, the right of the general public to know, by means of an overview file, the degree to which society is computerized, the relationships between the files, their concentration, etc.;
- then, although a number of legislations abandon or restrain it, the right for each individual to know that he is on file, in order to permit him, should he later so wish, to know the basic data (not the inferred results) figuring under his name on computer file
- finally, the right of the person on file to require from the holder of the file or his representative the rapid correction or erasure of certain data, with the help, if necessary, of the authorities responsible for data protection.

B. Evolution of the Right of Access

21. If the right of access is a collection of new subjective rights, correcting a right of property that seems to have been granted what may be feared as excessive power by the new technologies, certain recent developments in those technologies, **which further emphasize the non-controllability by the individual of the circulation of information** concerning him, have led some to further bestow the right of access, as it has already been consecrated by data protection legislation, with even more new subjective rights. Technological progress has created new modes of information collection that are more insidious because they are less transparent. Either they are more automatic because they are linked to a telematic service (electronic sales or credit terminal, computer mail catalogue, etc.), or more dangerous because they are linked to a service in the public interest such as the telephone. Two debates relayed to us by the authorities for data protection, the first, basically German, concerning the new additions to the telephone service offered by the RNIS, the other relating to memory or 'smart' cards used in the field of health care, serve to illustrate this

evolution of the right of access.

22. As regards the new additions to the telephone service offered in the framework of the RNIS, the discussion in the GFR has demonstrated the necessity of promoting the preliminary information of telephone subscribers in order that they can exercise their right of **informed consent** to certain options made possible by integrated network service technology, such as the identification of the caller's number, detailed accounts, and the appearance of the subscriber's name and qualifications in an electronic directory.

The **right to transparency** in the circulation of information consists essentially in the obligation of the operator and of everyone involved in the carrying out of the service, and for the host computer manager to inform the subscriber of all recording, processing, storing or transmission of nominative data concerning him, prior to their collection. This right to transparency is backed up by a right of **the free and informed consent** of the subscriber at various stages: in the case of the sampling of nominative data, this would involve the right not to be recorded in the directory and to demand the non-divulgence of the subscriber's number; it would equally involve the right to demand or refuse the automatic delivery of detailed accounts and the non-appearance of his number on the other's terminal. Finally, a legitimate complementary claim to the first two, **the right to anonymity**, the right to demand that techniques be put into service (for example, prepaid anonymous cards), permitting the anonymous utilisation of a public interest service, such as the telephone.

23. The non-transparence of data memory cards which incorporate a microprocessor, has given rise, in the health care field at least, to certain recommendations of the French CNIL deriving from the results of their experiments with 'Health' cards. Three principles apply:

- *that of voluntarism*: patients and doctors may not be forced to participate in the setting up of a data processing system. Neither advantage nor disadvantage may be the result of a refusal to participate;
- *that of free and informed consent to the use of the card*: patients and doctors must be clearly informed of the ends and means of the system, the methods of inscription and erasure of data, the persons authorized to read that information, and the guarantees, rights and recourse to justice at their disposal;
- *finally, that of the exclusion of all discrimination*: the principle of free choice of doctor by the patient and the principle of choice of medical practice may not be made an issue in any way.

Thus, the creation of new methods of collection, conservation and dissemination of information may enlarge the meaning and importance of the right of access, conceived, like all such measures, with a view to permitting the person on file to control the circulation of information concerning him.

III. THE EXPLANATORY BASIS ATTRIBUTABLE TO DATA PROTECTION LEGISLATION, JUSTIFIES, AT ONE TIME, BOTH THE FILE HOLDER'S RIGHT TO INFORMATION AND THE LIMITATIONS ON THIS RIGHT

A. Explanation

24. The individual is not the owner of data that concerns him, not even the bearer towards it of a right close to a real right. An individual projects a certain image of himself spontaneously upon society, which image may be precisely captured by another. Coupled with other information, it then takes shape in the eyes of the person who is processing it. There can be no question of a priori denying to another the use of an image of me which I myself have given him. My liberty is opposed to his, which is that of freedom of association within the framework of data systems operated by a union, of religious liberty in the framework of processing undertaken by a religious authority, or, more frequently, the liberty to do business in the case of companies. This conflict of liberties should resolve itself by the balance of interests method, by which the authority charged with deciding the conflict takes into account the respective legitimate interests expressing the liberty of each party.

We shall return to this point, but note at this stage that a number of legislative rulings foresee an exception for certain data or certain types of processing. Thus it is easy to justify, that legislation should forbid the processing of philosophical, trade union or religious data, because, a priori, the processing of such data imperils my religious, political or philosophical liberty. With reference to the same data, the same legislations exempt precisely such religious associations, trade unions and the press from this very prohibition, which can be explained by the desire to affirm the freedom of association and the freedom of the press above individual liberties. As we can observe from these limited examples, recording of the same nominative data may be limited, regulated, or free, according to the liberties put into question by its being recorded. There is certainly a debate between liberties and the necessity of appreciating, with regard to the interests of society, the weight accorded to each of them.

Particularly in the context of the freedom of the holder of the file to do business, beyond the limits imposed with regard to certain data which characterize, in an immediate way, such recognized constitutional liberties as freedom of opinion, of religion or of association, may we admit that legislation, in defining the file holder's right to information also defines the limits of that right? Should not the principle of the holder of the file's right to collect data be affirmed as such, even if, a posteriori, certain abuses must be decided in casu by the judge? In other words, should data protection legislation intervene in the private sector other than by providing for the right of access (see on this point para 18 etc.), should it rule on the contents and limits of private processing? The answer to this question may be clarified by studying the principles of regulation on public sector processing.

25. The right of public authorities to collect and process data can be explained by a fundamental liberty which in itself justifies that right. The decision of the Bundesgerichtshof previously cited explains the well-founded nature of this right and draws its conclusions as follows: "This 'right to self-determination in the matter of information' includes certain restrictions. The individual has no absolute right, that is to say he exercises no absolute sovereignty over the matters that concern him; his personality develops within the bosom of a social community, he cannot live without that community. Information, even of a nominative order, is a representation of social reality which is not uniquely the property of the individual concerned. As the jurisprudence of the Bundesverfassungsgericht has stressed several times, fundamental law resolves the individual-society dichotomy by considering a person as an entity joined with and inserted into society (...). This is why, in principle, an individual must accept restrictions on his 'right to self-determination in the matter of information' in favour of the preponderant general interest." These restrictions on the right of self-determination necessitate meanwhile a clear legal base in conformity with the constitution, and must, apart from that, respect the principles of clarity of norms and proportionality. In that which concerns electronic information processing, this signifies concretely: "Faced with the danger inherent in electronic information processing already described, legislators must take far more ample measures than previously with regard to the organization and procedure of data processing, in order to avoid any violation of anyone's human rights (...)." (BURKERT, 1985)

Public authorities' right to information, indispensible to the assurance of effective public service, necessitates respect for **the three principles of legality, speciality and proportionality.** These three principles have the following significance:

- **the principle of legality** requires that all data banks be created under legislative control, that is to say that the principal elements of regulation be defined by a law in the formal sense of the term. In a general way, this principle implies a certain coordinaton and control by the legislative body of the computerization of the public sector. It may be noted, that apart from the problem of individual liberties, a certain equilibrium of power is thereby re-established. The growing use of computerization in the public sector reinforces the active powers of the Executive and modifies the balance of power, an essential guarantee of democracy. The rejoining of the authority for the control of data protection with the Legislative and the considerable right of seizin accorded to the Legislative attached to that authority shares the same idea.
- **the principle of speciality** requires that the legislator indicate precisely the proposed use of nominative data and the persons for whom the collected data is destined. Thus an administrative authority may not record data except within the framework of a mission with which it has been

charged and inasmuch as that task is necessary for the public good or for the protection of citizens' interests **(principle of proportionality)**. A consequence of these two principles is, that within administrations, "one must be careful that processing programmes which serve different finalities are not interconnected. One must assure that each distinct area of administrative activity remains clearly separated and backed up with an interdiction to communicate data between the different sectors of activity: the executive power must also see to the creation of closed information systems... The general principle of separation of powers would thereby be complemented by a **'separation of powers as regards information'**" (BURKERT, 1985).

26. The **consecration of parallel principles** to those developed for the public sector, permitting the *rights of private holders of the file* to be restrained, is normal in West European data protection legislation. It might surprise the North American observer, who excludes private sector processing from the field of data protection legislation. The parallel European application of norms governing relations between citizens and public authorities can be explained by the fact that the State goes beyond its traditional constitutional role. "To its traditional duty to abstain, simply accompanied by the general obligation to maintain order, is added, nonetheless, the duty to take such measures as may be required to safeguard fundamental rights, to which function belongs also the satisfactory regulation of private judicial relationships." (RIGAUX, 1988, 489)

This extension of the role of the state justifies the explicit or implicit consecration in West European legislations of the principle of pertinence, applicable to files in the private sector and parallel to that already described with regard to files in the public sector.

27. In the private sector, the TRICOT report concludes that "the service expected of the company responsible for data collection is at once justification and limit of the use of the information". This principle of pertinence is taken up also by German, Austrian, Danish, Norwegian and Dutch laws.

As basis for the necessary consecration of this principle lies the following observation: "One must not lose sight of the fact that data is always gathered, memorized and communicated for a predetermined purpose. It is only by knowing that purpose, and not by abstract reasoning upon the actual data itself, that one may define the limits of tolerance acceptable to those involved." (TRICOT report)

Some people object to the lack of precision in this principle. The notion of 'pertinence', they say, is singularly vague and its use creates the risk of too wide an interpretation. This criticism seems to us to have little foundation. The criterion for 'pertinence' is certainly more flexible and more suited to evolving judicial summaries than an a priori ruling, drawing on the so-called 'per se' nature of the data, a criterion which, on the contrary, has *little regard for*

contractual reality.

It is clear that this principle is inapplicable when data is recorded without any contractual relationship, as in the case of compilers of mailing lists, 'head hunters' and agencies for commercial information. Such file holders are carefully distinguished from other private sector files and are the object of a priori regulations under the majority of European legislations.

28. The 'right to information' of companies and administrations involves them in certain consequences with regard to the utilization of data.

They are responsible for the security of their files. Article 7 of the Convention of the Council of Europe states: "... that appropriate security measures be taken to assure the protection of data against accidental destruction as well as against unauthorized access, modification or diffusion".

This question of security demands:

- the consecration of ethical codes applicable to any persons having any thing to do with data banks;
- for localized processing centres, the nomination of 'managers', whose statute should be similar to those of watchdog commissions, that is to say, persons charged with overseeing that the regulations concerning information are adhered to within companies and administrations;
- the progressive delineation of national and international norms of security for programmes processing nominative data.

Companies' and administrations' rights to information should be carefully distinguished from the *right of communication*. "The ruling suggested above, bearing on the principle of pertinence", explains the TRICOT report, "implies that information in the possession of a company and gathered under the aegis of a particular contract, may not be transmitted to third parties." Thus, according to German law, a company has no right to data communicated by another company, unless used in conformity with the stated contractual goals of processing. Furthermore, such use should be accountable to the first company and justified by the protection of the legitimate interests of that company on its own authority or the authority of a third party.

B. Evolution of Principles

29. The very foundation of the regulation of computer processing involving nominative data justifies a different appreciation of the principle of finality or pertinence, taking into account the new risks attached to recent technological developments. To be brief, two examples should suffice: expert systems and processing taking place within the framework of telematic operations involving the general public.

a. The Finality Principle and Expert Systems

30. The development of artificial intelligence or expert systems suggests certain reflections on the principle of finality. Such systems freeze a form of human reasoning into an automatic procedure: thus, an expert system enables one to evaluate the solvency of someone asking for credit, or to deduce certain complementary information concerning a consumer or group of consumers from a minimal data base.

It is traditional to recall, with regard to such systems, the ruling laid down by article 2 of the French law, according to which "no administrative or private decision involving a judgement of human behaviour may have as its sole basis an automatic data process giving a definition of the profile or character of the person concerned." Two reflections would seem to us to complete this legal reference. Firstly, the use of expert systems to identify not only individuals, but also groups of individuals, justifies the extention of the prescript to include processing programmes relating to groups of individuals. Secondly, it would be sensible if the person concerned could be warned of the existence of such an expert system, and of its use as a tool to assist decision making, and that a control of the quality of the system could be undertaken a priori (licensing system), or when ordered by a court.

b. The Finality Principle and Telematic Services Aimed at the General Public

31. The analysis of ruling prescripts, projected (such as the American EFT Privacy Act) or already adopted, relating to **telematic services**, leads to other reflections on the principle of finality. The first and most important, displays the a priori definition through the types of processing permitted by regulation to those who offer such services. Thus, article 9 of the German Bildschirmtextvertrag (computer text contract), applicable to videotext services to the general public, prescribes that the host may not handle data except for the purposes of billing and statistical understanding of his customers. It forbids the transfer of data to third parties, or the establishing of a customer character profile, except with the latter's permission. It limits the length of time that data may be conserved.

This tendency to define a priori the content of pertinent data, the length of its conservation and the types of legitimate use, may offend those people favourable to a free definition by companies, the actual file owners, of the finalities of processing, and who would prefer an *a posteriori control* at the discretion of a judge or an authority charged with surveying the legitimacy of processing goals. This principle of a posteriori control has been adopted by numerous legislations, notably the German, Austrian, Danish, Norwegian, etc. Making an issue of the principle concerning interactive services aimed at the general public seems to us to proceed from reawakened fears provoked by the nature of the recorded data and the method by which it is gathered.

32. The second reflection has to do with the prohibition of certain telematic services, such as the exclusion of opinion polling in the home. In the same spirit, certain processing should be forbidden, as for example the processing of data created by the use of video games, inasmuch as their processing can reveal the psychology of the user.

33. The third is the distinction in operation between, on the one hand, the **partners** to a service; he who offers the service, and he who receives the right of user and, on the other hand, those who collaborate in the realization of the service; which, in the case of E.F.T. (the American draft, E.F.T. Privacy Act), qualifies as 'E.F.T. Service Provider', that is to say, tradesmen on whose property terminals are installed, host centres common to more than one presenter of the service, transporter, etc.

The regulation of processing undertaken by this second category of persons is more severe. Their right to hold data within the framework of their mission is strictly limited, and not only the commercialization of data, but equally the establishment of information pools which could be useful to members of the network is forbidden. One finds here a distinction at work in certain legislations (e.g. the German, Austrian and Danish), which separates those companies processing data for someone else. These are subject to more rigorous regulations (rule of authorization).

IV. The explanatory basis attributable to data protection requires the recognition of a place of negotiation and arbitration: the role of data protection authorities

34. Burkert (1984) defined the preferable regulatory approach to computer technology (Information Law or Law of Information Technology) as follows. He refers to **'learning systems'**, that is to say, a legislative solution which, in the framework of a regulatory system, establishes "an institution provided with competence to collect the information in the regulated area, to make ad-hoc decisions according to rather more generally formulated criteria in a law and to feed back the information collected during the execution of its tasks to society and its role making agencies." Thus, the system is capable of learning and adapting, concludes the author. It is clear that the role given by our West European legislations to **data protection authorities** corresponds to this wish. Such authorities have multiple roles: "watchdog to assure the legitimacy of action of those who collect, process or distribute information (task fulfilled either by means of general or specific authorizations and/or by means of an investigatory power); consultative body for the public sector and sometimes even for the private sector, one of its goals being to promote practices suitable to all by setting up rules relative to the circulation of information; an institution in law or for the resolution of litigation; a body with independent powers to create norms and having at its disposition the necessary competence to adapt

the principles affirmed in law." (RODOTA, 1984)

35. It is clear that this conception of data protection legislation and the importance of the central role assigned to data protection authorities, meshes in perfectly with the proposed analysis; cannot data protection regulations be summed up in the debate we have described between the liberty of the file holder and that liberty endangered by his liberty, that of the person on file? This debate cannot be resolved once and for all. Its solution demands that the authority charged with arbitration be able to weigh the interests at stake, and this with regard to a technological evolution that renders it impossible to freeze a particular solution, but obliges one to evaluate how much the latter will alter the fragile and barely defined equilibrium (see, in this context, the evolution previously documented, promoted by data protection authorities; the right of access and the finality principle).

36. Thus, the essential role of data protection authorities is to be a **place of dialogue and negotiation**. In France, the system of simplified norms discussed with sector representatives appears to be a flexible and unconstrained way promoting rules of conduct adapted to the specific needs of that sector. The solution devised by recent Dutch legislation, and the practice of the Data Protection Act inspired by the same principle, permit a sector to elaborate its own codes of conduct whose ratification is afterwards negotiated with the commission for data protection. If the new role of data protection authorities appears to us to be indispensible and in need of enlargement, the fact of only finding one of the parties at the negotiating table, namely the file holders, and the fear that these could organize themselves on precisely such an occasion in order to defend a common position, causes one to fear that the resulting arbitration could be falsified to their advantage. In this respect, the openness of these debates and the representation in them of the persons on file are unavoidable requirements if the data protection authority is to become the patron of a dialogue between the persons on file and holders of the file and help both parties to define a more congenial, more habitable information society.

Concise bibliography

J. Bing, "International Services Bureaux and T.D.F.", *Complex* 1/85, Norwegian University Press, Oslo.

Bing, *Impact of Developing Information Technology on Data Protection Legislation*. Report prepared for ICCP, OCDE, 1986.

H. Burkert, "The Law of Information Technology – Basic concepts, Colloque de l'ABDI, Computer and Telecommunications," *Is there a lawyer in this Room*. 7–10 Dec. 1987, Travaux et Précis de la Faculté de droit de Namur, Ed. Story Scientia, Bruxelles, no. 8, 1989.

H. Burkert, "Information Law and Information Ethics, La télématique", *Actes du colloque de Namur*. Travaux et Précis de la Faculté de droit de Namur, Ed. Story Scientia, Bruxelles, 1983, T.C.

H. Burkert, *Datenschutz und Informations- und Kommunikationstechnik: eine Problemskizze* (Bonn, GMD, 1985).

H. Burkert, "Institution of Data Protection – An attempt at a functional explanation of European National Data Protection Laws", *Computer Law Journal*, 1982, vol. 3, no. 1, 169 ff.

J.L. Brown, "Implications of the informal nature of payments", *Computer Law Journal*, 1980, 2, 153 ff.

P. Catala, "Ebauche d'une théorie juridique de l'information", *Rev. dr. prospectif*, 1983, no. 1.

"CNIL, 10 ans d'informatique et libertés", *Economica*, Paris, 1988, 96.

D.H. Flaherty, *Protecting Privacy in Two ways Electronic Services*, (London, Mansell 1985).

D. Froystad, "Data protection in practice: identifying and matching elements, Teresa (17)", Complex NRCCL, Oslo, 1984 Complex 8/84, Norwegian Univ. Press, Oslo, 1984.

H. Godschalk, "Datenschutz am point of sale", *Computer und Recht*, 1987, no. 7, 416 ff.

I.B.I., *De l'informatique juridique au droit de l'informatique*, Document, DR 09, Jan. 1983.

D.A. Marchand, "Privacy, Confidentiality and Computers: National and International Implications of U.S. Information Policy", *Telecommunications Policy*, Sept. 1979.

Office of Technology Assessment (O.T.A.) Selected Electronic Fund Transfer Issues, *Privacy, Security and Equity*, Background Paper, Congressional Board, 94th, Congress, 1982.

Office of Technology Assessment (O.T.A.) Electronic Surveillance and Civil Liberties, Congress of U.S., Washington, 1985.

Y. Poullet, "TEF et protection des données à caractère personnel", Rapport présenté au 6ème séminaire de droit à la consommation, EFT and Consumer Protection, I.I.N. 1987.

Y. Poullet, "Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information", Conseil de l'Europe, Conf. d'Athènes, Nov. 1987, publiée D.I.T., 1988.

Y. Poullet and F. Warrant, "Nouveaux compléments au service téléphonique et protection des données: A la recherche d'un cadre conceptuel". Rapport au Conseil de l'Europe. Jan. 1989.

F. Rigaud, *La protection de la personne et de la vie privée*, Précis, UCL, Faculté de droit, 3 tomes, 1988.

S. Rodota, "Protection de la vie privée et contrôle de l'information: deux sujets d'inquiétude croissante pour l'opinion publique, Questions d'ordre politique soulevées par la protection des données et des libertés individuelles", OCDE, *Etudes d'informatique*, no. 10, Paris, 1976.

S. Rodota, "The Social Challenge of Information Technology, 1984 and beyond", *Colloque de l'OCDE*, Berlin, Nov. 28–30, 1984.

S. Rodota, "Protezione dei dati e circulazione delle informazioni", *Riv. Crit. del Diritto Priv.*, 1984, no. 4, 721 ff.

J. Schneider, "Datenschutz und Neue Medien", *NJW* 1984, 390 ff.

A. Westin, "Privacy issues and the implications of home banking", *American Banker*, June 3, 1981.